Names and the FPKI Directory Strategy

Bill Burr
NIST
william.burr@nist.gov
August 10, 2000

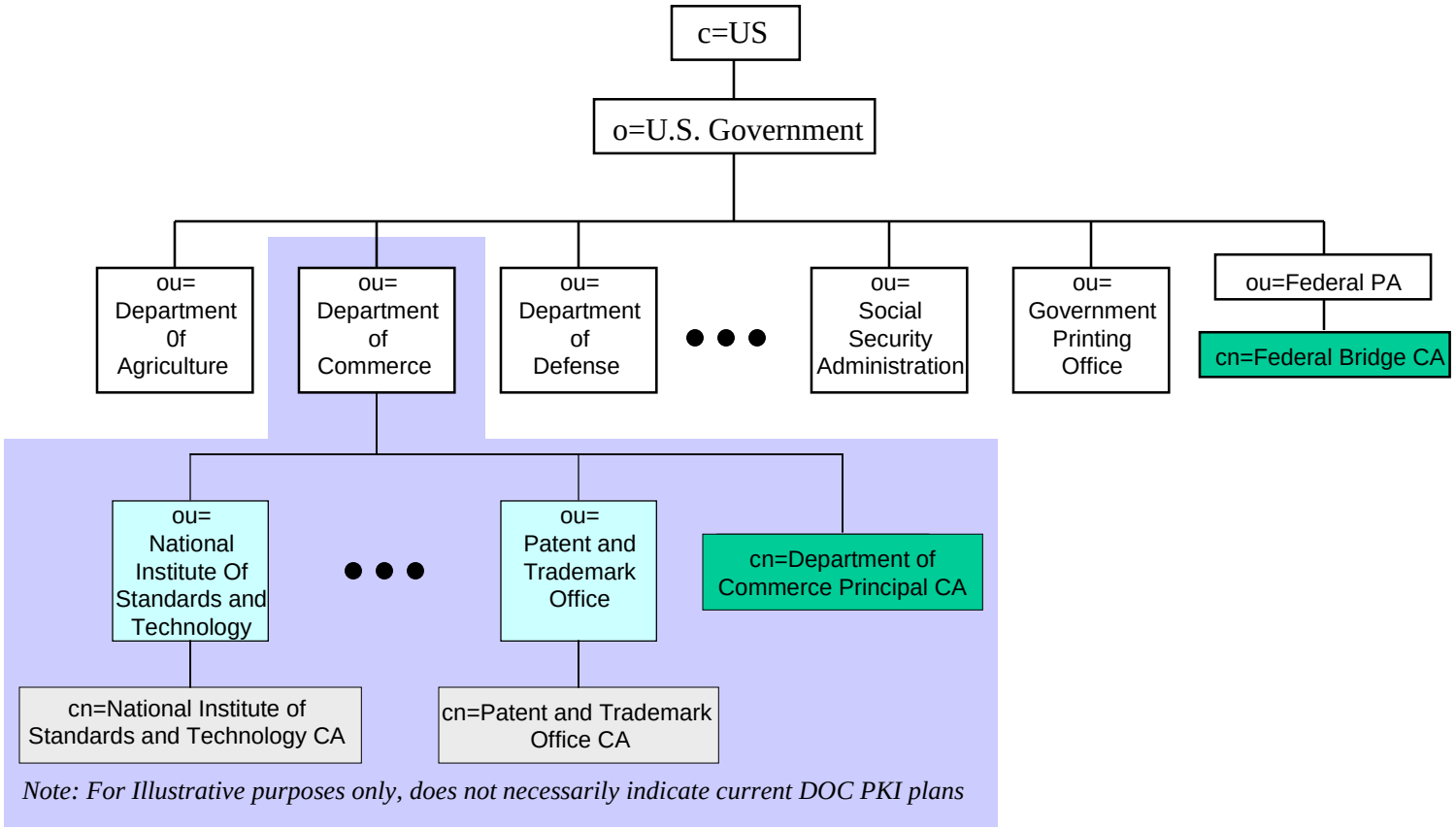
Names in a PKI

- Names have to be unique
- Names ought to be meaningful, but
  - Too much semantic content may not be good
    - Name changes can cause big problems if the names are burned into certificates
      - Agency structure is not static
        - » SSA used to be part of HHS
      - Names change
        - » NIST used to be NBS

X.500 Distinguished Name

- c=US
- o=U. S. Government
- ou=Department of Commerce
- ou=National institute of Standards and Technology
- cn=National Institute of Standards and Technology CA

Conventional X.500 Names and DIT



Name Registration

- Need a registrar
  - unless we literally accept the names and structure in FIPS 95, or the US Government Manual
  - GSA has the responsibility
  - Policy Authority could register names as a part of the application process, so this might not be a big deal

USGold

- Refers to US Gov. Manual & FIPS 95
- FIPS 95
  - Structure for reporting financial data
    - Executive
    - Judicial
    - Legislative
    - Quasi-Federal
    - International

X.500 DN Advantages

- Structure can be meaningful
  - If we use FIPS 95 names they will be meaningful for financial purposes
- Might facilitate use of name constraints
- Pretty conventional in OSI terms
  - Allied governments, DoD use something like this, etc.

X.500 DN Disadvantages

- Who knows or uses these names?
- Not aligned with the Internet Domain Names
- Need a registrar of names
  - Somebody at GSA?
- Despite original intention, not a global infrastructure:
  - No global root directory
  - We'll have to set up a UG gov. root for PKI

Internet Domain Names

- Familiar structure
  - www.nist.gov,
  - cio.treas.gov,
  - amazon.com
- A hierarchy, but usually pretty flat
  - www.irs.treas.gov about as deep as it gets
- Domain Name Service resolves them into 32-bit IP address by a referral process
  - 192.248.32.14

Internet Domain Names

- An existing, global naming infrastructure
- Agency have Internet Domain Names
  - We more or less know what they mean
- Fed. personnel have RFC822 e-mail addr.
  - Usually includes agency domain name
    - william.burr@nist.gov
- More or less everybody in the world now uses the Internet and domain names

Domain Name Service

- An existing global directory system:
  - As wide as the internet
    - we know it scales
  - Resolves Internet Domain Names to binary IP addresses
    - www.something.com becomes 192.248.32.14
  - Based on referrals
  - SRV REC will provide addresses of services associated with each domain

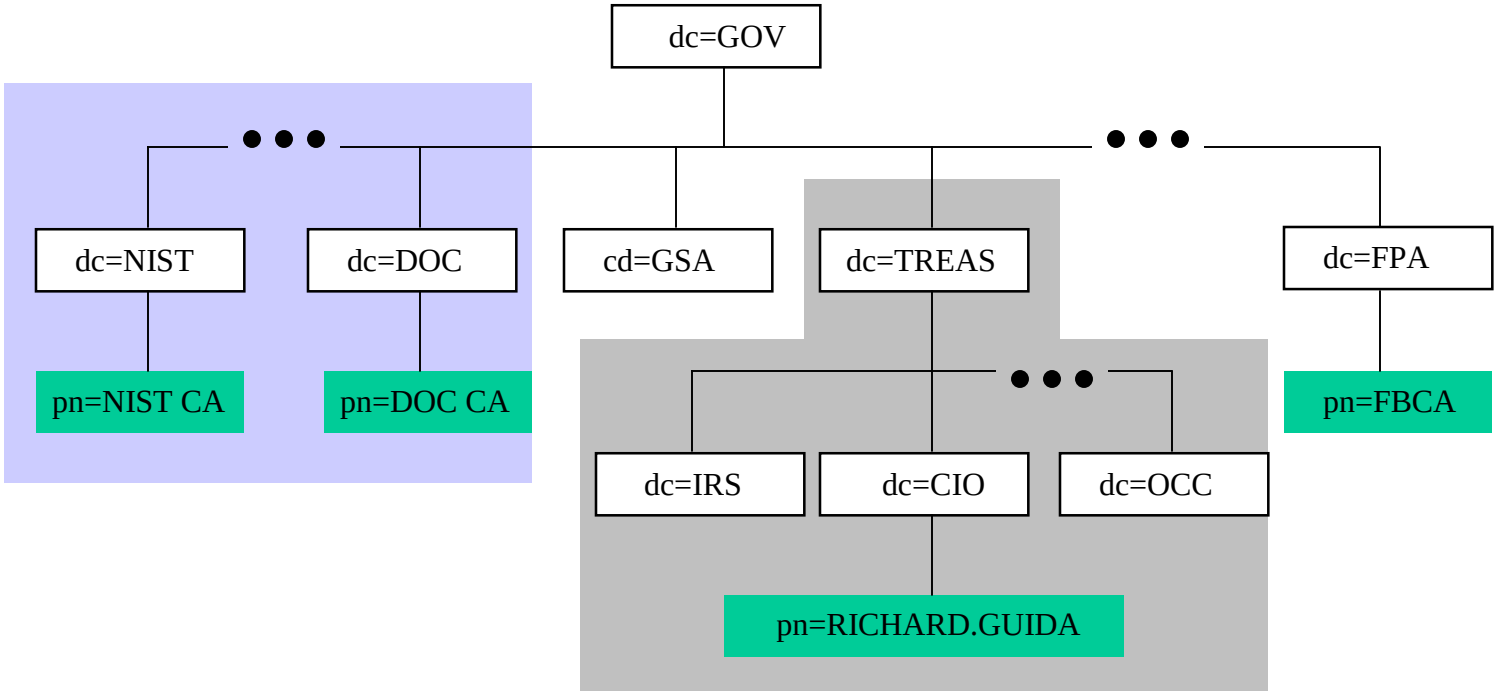
Domain Name Disadvantages

- Usually not much structural information
  - May limit utility of name constraints
  - Names are unique, but not as informative as they might be
  - May also be an advantage
- May fly in the face of established directory arrangements in some agencies and with other countries

Domain Component Names

- A way to introduce domain names into the X.500 information model
- RFC 2247 & RFC 2377
- John.Smith@irs.treas.gov becomes:
  - ***dc=irs, dc=treas, dc=gov, uid=john.smith@irs.treas.gov***
- Question: can current pki clients build paths from domain component names?
  - If not when?

Domain Component Naming DIT



A Strategy

- Accept that, for a while at least, we're stuck with both: we aren't going to resolve this now
- Two parallel, more or less independent directory trees
  - Traditional X.500 DNs
  - Domain component based naming

Two Kinds of Directory Servers

- X.500 DSA
  - Supports LDAP (hopefully v3) client interface
  - Supports DSP chaining of directory servers
- LDAP servers
  - Supports LDAP v3 client interface
    - LDAP v3 referrals
  - Chaining, if offered, is proprietary
- Both support the same X.500 directory information model

Client Assumptions

- PKI clients can build paths that use either naming style, or both
  - Of course some clients today can hardly build paths at all
- PKI clients use LDAP v3, and this means referrals

X.500 DN Realm

- X.500 domain names
  - GSA registers names
- Use X.500 DSAs
- FBCA operates root for o=US government
- Agency border directories chain to FBCA directory
  - tough to set up, but relatively simple to maintain once established
- Clients use LDAP
  - Hopefully v3 with referrals

DCN Realm

- Domain Component Names
- Use LDAP servers
  - Must support LDAP v3 and referrals
- Agency border directories refer rather than chain
  - Easy to setup, but maybe hard to maintain
  - DNS SRV RECs may help
  - Automatically refer to FBCA directory?

How do we cross realms?

- For clients in the DCN realm
  - Referral to FBCA DSA should work;
    - A more direct referral might be better, but who will maintain the knowledge base?
- For clients in the X.500 realm
  - FBCA directory is meta-directory that turns chained queries into LDAP queries, or;
  - Can X.500 DSAs generate referrals for DCN names??????

FBCA Directory

- Root for o=US Government
- Supports X.500 chaining
- May need to be a meta-directory capable of resolving chained queries for DCN names through LDAP
- May need to maintain knowledge base for referrals within the DCN realm
  - Perhaps a separate LDAP server
  - Will DNS SRV Recs save us?

Some Issues

- Can PKI clients build cert paths with DCN names?
- Can X.500 DSAs generate LDAP v3 referrals for DCN names?
- Can we make name constraints work across the gulf?
- Is SRV Rec support ubiquitous in the DNS?

My Belief

- X.500 chaining is fairly mature and works; we'll get this running first, but
- DCN naming (or else something based on domain names) will prevail in the long run and at large, because our PKI, names and directories need to be aligned with the Internet, not orthogonal to it.